UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/737,374	12/16/2003	Roger Hansen	200312027-1	5369

22879 7590 03/01/2011

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
TRUONG, LOAN	

ART UNIT	PAPER NUMBER
2114	

NOTIFICATION DATE	DELIVERY MODE
03/01/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/737,374
Filing Date: December 16, 2003
Appellant(s): HANSEN ET AL.

Hansen et al.
Hewlett-Packard Development Company, L.P.

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed December 6, 2010 appealing from the Office action mailed September 20, 2010.

1. **Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

2. **Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. **Status of Claims**

The statement of the status of claims contained in the brief is correct.

4. **Status of Amendments After Final**

No amendment after final has been filed after the Office Action of September 20, 2010.

5. **Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

6. **Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

7. **Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

8. **Evidence Relied Upon**

7,165,186	Viswanatham et al.	October 7, 2003
6,941,410	Traverstat et al.	June 2, 2000
7,222,194	Kano et al.	July 17, 2003
6,691,245	DeKoning	October 10, 2000

9. **Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

a) Claims 1-8 and 39-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Viswanatham et al. (US 7,165,186) in further view of Traversat et al. (6,941,410) in further view of Kano et al. (US 7,222,194).

In regard to claim 1, Viswanatham et al. teaches a system for storing checkpoint data comprising:

a persistent memory unit (backup store may be located on a separate computer from nodes 120A-B, fig. 1, col. 3 lines 53-56) coupled to the network interface (network may be a LAN, WAN, the internet or other types, col. 2 lines 63-67), wherein:

the persistent memory unit (backup store, fig. 1, 150) is configured to receive the checkpoint data into a region of the persistent memory (persistent store maybe able to store the current state of various active components, col. 3 lines 38-42) via a remote memory write command (execution of active component operate checkpoint mechanism to take checkpoint and store to persistent store, col. 4 lines 5-10) from a primary process (active application, col. 3 lines 20-28) through the network interface unit (network may be a LAN, WAN, the internet or other types, col. 2 lines 63-67) and provide access to the checkpoint data in the region via a remote read command (if server 130C fails sever 130B may be able to retrieved the saved state of component 144B, col. 4 lines 10-16) from a backup process (backup application, col. 3 lines 20-28) through the network interface (network may be a LAN, WAN, the internet or other types, col. 2 lines 63-67); and

backup process provides recovery capability in the event of a failure of the primary process (in the event of a server failure, the data objects may be retrieved by fail-over components on another server, col. 1 lines 35-41).

Viswanatham et al. does not explicitly teach a persistent memory unit configured to receive or access data via a remote direct memory write/read.

Traversat et al. teach of a virtual heap for a virtual machine by implementing a virtual heap maintained on non-volatile memory storage external to the device running the virtual machine (abstract) and the virtual persistent heap enable the migration of the virtual machine computation states and thus the migration of executing processes from one machine to another (abstract, fig. 5a) implementing a paging-based approach which

may enable page protection mechanisms and support for DMA and block I/O devices (col. 19 lines 23-31).

It would have been obvious to modify the system of Viswanatham et al. by adding Traversat et al. virtual heap. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would further teach the uses of the data in the persistent memory enable the check-pointing of the state of the computation of a virtual machine including processes executing within the virtual machine to a persistent storage (abstract).

Viswanatham et al. and Traversat et al. does not explicitly teach a network interface to an external network; and a persistent memory unit wherein the memory write command is preceded by a create request for the region and the read command is preceded by an open request for the region.

Kano et al. teach of a backup system constituted of a network attached storage (NAS) (col. 3 lines 7-15) wherein the NAS constituted of a network interface for connection to LAN (fig. 1, 110) wherein when a file access is for data write the NAS assigns a new data block for storing data (col. 10 lines 7-26) and when reception of an open command the backup server issues a file open request to the NAS (col. 9 lines 63-67).

It would have been obvious to modify the system of Viswanatham et al. and Traversat et al. by adding Kano et al. backup system. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would clearly show a connection of network such as a LAN

through a network interface (fig. 1, 110) and further clearly describes method of file accesses (col. 9 lines 43-67 and col. 10 lines 1-34).

In regard to claim 2, Viswanatham et al. does not explicitly teach the system of Claim 1, further comprising: a persistent memory manager configured to program the network interface with information used by the network interface to perform virtual-to-physical address translation.

Traversat et al. teach the virtual heap with a page table and offset based address translation may be used to convert virtual heap references into in-memory heap references (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

In regard to claim 3, Viswanatham et al. teach the system of Claim 1, wherein the persistent memory unit is configured to provide remote memory read to the checkpoint data to another processor, and the backup process is executed by the other processor (if server 130C fails sever 130B may be able to retrieved the saved state of component 144B, col. 4 lines 10-16).

Viswanatham et al. does not explicitly teach the system wherein the persistent memory unit provides data through a remote direct memory read.

Traversat et al. also provide paging-based approach which may enable page protection mechanisms and support for DMA and block I/O devices (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

In regard to claim 4, Viswanatham et al. teach the system of Claim 1, wherein the persistent memory unit provides the checkpoint data through remote memory reads by the backup process after the primary process fails (in the event of a server failure, the data objects may be retrieved by fail-over components on another server, col. 1 lines 35-41).

Viswanatham et al. does not explicitly teach the system wherein the persistent memory unit provides data through a remote direct memory read.

Traversat et al. also provide paging-based approach which may enable page protection mechanisms and support for DMA and block I/O devices (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

In regard to claim 5, Viswanatham et al. does not explicitly teach the system of Claim 1, wherein the persistent memory unit is configured to store multiple sets of checkpoint data through remote direct memory writes sent from the processor at successive time intervals.

Traversat et al. teach of a checkpoint be induced after a maximum elapsed time (col. 24 lines 42-47). Also, Traversat et al. provide paging-based approach which may enable page protection mechanisms and support for DMA and block I/O devices (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

In regard to claim 6, Viswanatham et al. does not explicitly teach the system of Claim 5, wherein the persistent memory unit provides the multiple sets of checkpoint data through remote direct memory reads upon request by the backup process at one time.

Traversat et al. teach of migrating a virtual persistent heap from one machine to another (abstract). Also, Traversat et al. provide paging-based approach which may enable page protection mechanisms and support for DMA and block I/O devices (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

In regard to claim 7, Viswanatham et al. teach the system of Claim 1, wherein the primary process provides the checkpoint data to the persistent memory unit independently from the backup process (persistent store maybe able to store the current state of various active components, col. 3 lines 38-42).

In regard to claim 8, Viswanatham et al. teach the system of Claim 1, wherein the persistent memory unit is configured as part of a memory access-enabled system area network (network may be a LAN, WAN, the internet or other types, col. 2 lines 63-67).

Viswanatham et al. does not explicitly a remote direct memory access.

Traversat et al. also provide paging-based approach which may enable page protection mechanisms and support for DMA and block I/O devices (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

In regard to claim 39, Viswanatham et al. does not explicitly teach the system of Claim 1, the persistent memory unit configured to provide access to the checkpoint data in another region via a remote memory read command from the backup process (sever 130B may be able to

retrieved the saved state of component 144B, col. 4 lines 10-16) through the network interface (network may be a LAN, WAN, the internet or other types, col. 2 lines 63-67).

Viswanatham et al. does not explicitly a remote direct memory access.

Traversat et al. also provide paging-based approach which may enable page protection mechanisms and support for DMA and block I/O devices (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

Viswanatham et al. and Traversat et al. does not explicitly teach the persistent memory unit wherein the read command is preceded by an open request for the another region.

Kano et al. teach of a file access is for data write the NAS assigns a new data block for storing data (col. 10 lines 7-26) and when reception of an open command the backup server issues a file open request to the NAS (col. 9 lines 63-67).

Refer to claim 1 for motivational statement.

In regard to claim 40, Viswanatham et al. does not explicitly teach the method of Claim 1, wherein the checkpoint data received by the persistent memory unit overwrites a current set of the checkpoint data.

Traversat et al. teach of persistent store space may include an entire copy of the virtual heap for one or more other applications (col. 10 lines 23-34).

Refer to claim 1 for motivational statement.

In regard to claim 41, Viswanatham et al. does not explicitly teach the method of Claim 1, wherein the checkpoint data received by the persistent memory unit is appended to a previous set of the checkpoint data.

Traversat et al. teach of persistent store space may include one or more versions of copies of virtual heap or checkpointed states (col. 10 lines 23-34).

Refer to claim 1 for motivational statement.

****

b) Claims 9 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Viswanatham et al. (US 7,165,186) in further view of Traversat et al. (6,941,410) in further view of Kano et al. (US 7,222,194) in further view of DeKoning (US 6,691,245).

In regard to claim 9, Viswanatham et al does not explicitly teach the system of Claim 1, wherein the persistent memory unit is configured with translation tables.

Traversat et al. teach the virtual heap with a page table and offset based address translation may be used to convert virtual heap references into in-memory heap references (col. 19 lines 23-31).

Refer to claim 1 for motivational statement.

Viswanatham et al., Traversat et al., and Kano et al. does not explicitly teach the system of Claim 1, wherein the persistent memory unit is configured with address protection to authenticate requests from remote processors, and to provide access information to authenticated remote processors.

DeKoning teach of a remote storage device which is initially fully mirrored from the local storage device before operations can start using the local host device (col. 7 lines 58-65).

It would have been obvious to modify the system of Viswanatham et al. and Traversat et al. and Kano et al. by adding DeKoning host-initiated and fail-over. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would provide the second host device upon failure of the first host device to initiate a switch or fail-over and server as the primary on behalf of the client devices (abstract).

In regard to claim 38, Viswanatham et al., Traversat et al., and Kano et al. does not explicitly teach the system of Claim 1, wherein the persistent memory unit is further configured to store meta-data regarding the contents and layout of memory regions within the persistent memory unit and to keep the meta-data consistent with the checkpoint data stored on the persistent memory unit.

DeKoning teach of a primary storage device stores data received from the host device responds to the storage access request and at a synchronize checkpoints forward the data and the synchronization checkpoint to the secondary storage (col. 4 lines 1-8).

Refer to claim 9 for motivational statement.

10. **Response to Argument**

Applicant points out that the 35 U.S.C. 103(a) rejections in regard to claims 1-9 and 38-41 over Viswanatham et al. in further view of Traversat et al. in further view of Kano et al. raised the following issues:

i. In regard to claim 1, appellant stated that the network 170 of Viswanathan et al. is not the path through which checkpoint commands flow. The office action relies on the backup store and a network interface of Viswanathan et al. with no network interface specifically shown and therefore must relied on an allegedly inherent network interface. Furthermore, the allegedly inherent network interface is reference by the office action on col. 2 lines 63-67 where the network 170 between the client devices 160 and the load balancer 110 but fig. 1 of Viswanathan et al. clearly shows the backup store having a separate connection to the nodes than the load balancer and network 170. Given the location of the backup store in relation to the network and load balancer, it seems clear that commands used to write checkpoint data to the backup store do not flow through the network and/or load balancer.

Examiner disagrees. Viswanathan et al. teaches of a distributed system with a plurality of servers that may be connected by a load balancer and a network where each server executes one or more application components and each application component may have one or more redundant backup components located on a separate server. In the event of a server failure, a redundant backup component may be activated and to maintain backup application components, the current state of

active application components may be checkpoint to a backup store (col. 1 line s20-41). For further clarification of the network interface in relation to the backup store, Viswanathan et al. teaches that the backup store maybe be located on a separate computer from nodes 120A-B (col. 3 lines 50-56). By definition, a network interface (network interface controller, network adapter, or LAN adapter) defined by wikipedia.org (http://en.wikipedia.org/wiki/Network_interface_controller) as "a computer hardware component that connects a computer to a computer network." While fig. 1 of Viswanathan et al. show the backup store without a network interface and being separate from the network 170, it is obvious that since the backup store is located on a separate computer and external to nodes 120A-B, this separate compute would required a network interface to connects itself to the computer network and nodes 120A-B. The commands used to write checkpoint data or read checkpoint data would then flow through the separated computer's network interface and hence read on the claimed limitations.

ii. Appellant argues that inherency fails for Viswanathan et al. in situation where the backup store is located on a separate computer from the nodes 120A-B, it is not necessarily present that the commands to write information to the backup node would flow through the load balancer and network 170 by fig. 1 different configuration paths for which data is written to the backup store and the load balancer/network 170.

Examiner disagrees. The inherency does not fail based on similar reason mention in section i. Refer above for more details.

iii. Appellant stated that Kano is relied upon by the Office Action, deals with file opening procedures not associated with initializing DMA. Furthermore, appellant stated that broadest reasonable interpretation cannot expand the DMA operation to file-level operations.

Examiner disagrees. The claim language does not exclude file-level operations or include initializing DMA but simply states “a remote direct memory write command is preceded by a create request and the read command is preceded by an open request." Viswanthan et al. in view of Traverstat et al. in view of Kano where Traverstat et al. is relied upon for the teaching of a remote direct memory command and Kano is relied upon to teach a file open or create process before a read or write is executed. Therefore, based on the broadest reasonable interpretation, Kano does in fact teach the claimed open and create process preceded a write or read.

iv. In regard to claim 2, appellant stated that the office action relied on an allegedly inherent teaching of Traverstat that the heap translation is performed by a network interface. However, the translation of Traverstat could be performed by an array of other devices, such as a main processor or the memory controller.

Examiner disagrees. Viswanathan et al. teaches a network interface in a distributed system where the backup store is located on a separate computer from nodes 120A-B (col. 3 lines 50-56) and Traversat et al. teaches a virtual heap with a page table and offset based address translation used to convert virtual heap references

into in-memory heap references and support for DMA (col. 19 lines 23-31). As define by wikipedia.org (http://en.wikipedia.org/wiki/Network_interface_controller), the network interface controller may implements DMA data transfer technique where an intelligent peripheral assumes control of the system bus to access memory directly where this removes load from the CPU but requires a separate processor on the card. The combination of Viswanathan et al. in further view of Traversat et al. would allow for a network interface implementing DMA capabilities. It would be obvious by wiki definition of a network interface that the network interface would be performing the heap translation using the DMA capabilities.

v. Appellant points out that the rejection of claims 9 and 38 over Viswanathan et al., Traversta, Kano and DeKoning are allowable for the same reason,

Examiner disagrees. Claim 9 and 38 are rejected for the same reasons above.

11. **Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Loan Truong
Patent Examiner
(571) 272-2572

/Scott T Baderman/
Supervisory Patent Examiner, Art Unit 2114

Conferees:

/STB/
Scott Baderman
SPE, Art Unit 2114

/RB/
Robert Beausoliel
SPE, Art Unit 2113